OKSHINE and HIPAA Update - 2023

PLICO Explore Healthcare Summit

Cori H. Loomis, JD
Christensen Law Group, PLLC

What we're going to cover

- OKSHINE and Interoperability Requirements
- Legal Medical Record v. Designated Record Set
- Record Retention
- Security Update and Cyber-Threats
- Part 2 Proposal

OKSHINE – Why?

Medicare & Medicaid E.H.R. Incentive Programs: 2011-2018

- Introduced in 2011 as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.
- Encouraged eligible professionals (EPs); eligible hospitals, and critical access hospitals to adopt, implement, and upgrade certified electronic health record (CEHRT) and demonstrate meaningful use of health information technology.

OKSHINE – Why?

- Medicare incentives ended in 2016 after passage of the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA).
- Medicare downward payment adjustments started in 2015.
- Renamed Promoting Interoperability in 2018.
- Medicaid incentives ended in 2021.

OKSHINE – Why?

Quality Payment Program

MACRA required CMS to implement an incentive program, referred to as the Quality Payment Programs, that provides two participation tracks:

MIPS
Merit-based Incentive Payment System

Advanced APMS
Advanced Alternative Payment Models

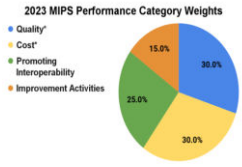
OKSHINE – Why?

Merit-Based Incentive Payment System (MIPS) in 2022 and 2023

*** Positive, negative or neutral payment adjustment**

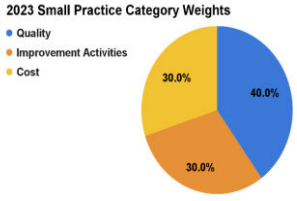
MIPS Performance Category	Percent of Total Score
Quality	30%
Cost	30%
Improvement Activities	15%
Promoting Interoperability	25%

OKSHINE
Why?



- Must reach 75 MIPS points in 2022 and 2023 to avoid a negative payment adjustment in the 2025 payment year.

OKSHINE
Why?

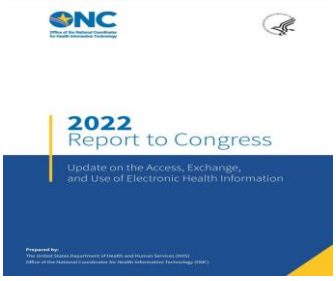


- Special scoring applies to small practices (15 or less) that may result in reweighting of the categories.
- https://qpp.cms.gov/mips/special-statuses?py=2023.

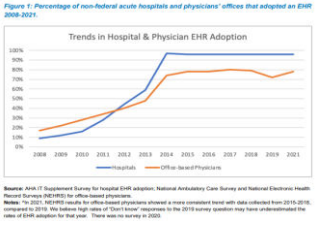
OKSHINE
Why?

- **Promoting Interoperability Performance Category Objectives and Measures**
  - Electronic Prescribing (State law requirement)
  - Health Information Exchange (Now state law also)
  - Provider to Patient Exchange
  - Public Health and Clinical Data Exchange
  - Requires 2015 Edition CEHRT, 2015 Edition Cures Update CEHRT, or a combination of both
  - https://www.healthit.gov/sites/default/files/facas/2022-01-19-CMS_Promoting_Interoperability_Program_Update_508.pdf.

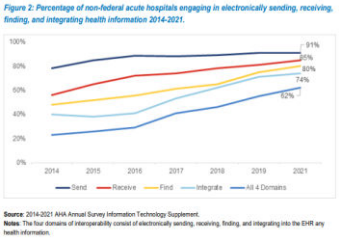
OKSHINE
Why?



OKSHINE
Why?

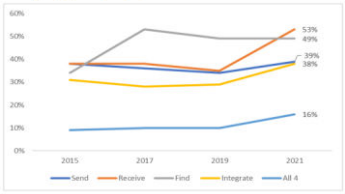


OKSHINE
Why?



OKSHINE Why?

Figure 3: Percentage of physicians engaging in electronically sending, receiving, searching/querying, and integrating any health information 2015-2021.



Source: National Electronic Health Record Survey, 2015-2021.
Notes: The four domains of interoperability consist of electronically sending, receiving, finding, and integrating into the EHR any health information.

OKSHINE Why?

- "An overwhelming majority (over 75 percent) of physicians who engaged in Health Information Exchange (HIE) experienced improvements in quality of care, practice efficiency, and patient safety."
  - ONC Report 2022

OKSHINE

SB 574 (May 2021) and SB 1369 (May 2022)

- Created the Oklahoma State Health Information Network Exchange (OKSHINE) and Office of the State Coordinator for Health Information Exchange.
- Declared a mandate that "all providers" participate in the statewide HIE by July 1, 2023.
  - Establish a direct secure connection to the SDE and transmit active patient data.
  - Actively utilize HIE services to securely access records during and/or in support of patient care.

MyHealth

In choosing MyHealth, an Oklahoma-based 501c3:

- >80% of Oklahoma's health care data already connected.
- ~400 organizations do not need to reconnect.
- Existing legal agreements and policies remain in place.
- Eligible for federal funding from CMS and other agencies.
- Extensive governance of network and data use.
- Providers and other health care stakeholders.
- State is a participant.

MyHealth

In choosing MyHealth, an Oklahoma-based 501c3:

- >80% of Oklahoma's health care data already connected.
- ~400 organizations do not need to reconnect.
- Existing legal agreements and policies remain in place.
- Eligible for federal funding from CMS and other agencies.
- Extensive governance of network and data use.
- Providers and other health care stakeholders.
- State is a participant.

OKSHINE Questions

- Are physicians who are licensed in Oklahoma, but who do not have a physical practice here required to sign up?
- What protected health information must be accessible through HIE?
- Funding?
- Exceptions?
  - Criteria for obtaining one?
- Penalties?
- Implementation?
  - NPP
  - Opt Out

OKSHINE Rules

- OHCA Board of Directors approved first set on March 22, 2023.
- Disapproved by Governor Stitt on June 23, 2023.
- Second set proposed as emergency rules.

OKSHINE Rules - Changes

- Anyone without an EHR is automatically exempted. (d)(2)(A)
- All substance abuse treatment facilities are automatically exempted. (d)(2)(B)
- All exemption request are automatically granted. (f)(2)
- All exemption requests are effectively permanent unless the provider withdraws the exemption. (f)(3)
- Providers will apply for a grant from OHCA for the connection fee. OHCA will pay that directly to MyHealth. (e)(3)

OKSHINE -Medicaid Manged CAre

- **1.21.8 Health Information Exchange**

As required by OHCA, the Contractor shall participate in the SDE-HIE for submission of Encounter Data and exchange of clinical information in order to improve the quality and efficiency of health care delivery in numerous ways, including: reducing medical errors, decreasing duplicative or unnecessary services. improving data quality for public health research, promoting population health management, reducing manual, labor-intensive monitoring and oversight, and reducing Fraud and Abuse.

OKSHINE -Medicaid Manged CAre

- **1.21.8 Health Information Exchange**
- The Contractor's participation shall include ensuring the compliance of their Participating Providers with 63 O.S. §§ 1-133. In addition, Contractor shall ensure that all Participating Providers comply with subsequently promulgated rules implementing said mandate. As it applies to this RFP, the Contractor's Participating Providers shall become compliant with 63 O.S. §§ 1-133 if not already compliant.

NPP Language

- **We may participate in digital health information exchanges with other health care provider members, in which we send patient data to a network system committed to securing the information and allowing your data to be available to another member who is providing treatment to you.**

Proposed HIPAA Rules

- Still waiting on final HIPAA rule.
  - RFI in December 2018
  - NPRM issued December 10, 2020
  - Supposed to be released in March 2023.
- Proposed Part 2 rule
  - December 2, 2022

Proposed HIPAA Updates

- Allowing patients to inspect their PHI in person and take notes or photographs of their PHI.
- Changing the maximum time to provide access to PHI from 30 days to 15 days.
- Restricting the right of individuals to transfer ePHI to a third party to only ePHI that is maintained in an EHR.
- Confirming that an individual is permitted to direct a covered entity to send their ePHI to a personal health application if requested by the individual.
- Stating when individuals should be provided with ePHI without charge.

Proposed HIPAA Updates

- Requiring covered entities to inform individuals that they have the right to obtain or direct copies of their PHI to a third party when a summary of PHI is offered instead of a copy.
- The Armed Forces' permission to use or disclose PHI to all uniformed services has been expanded.
- A definition has been added for electronic health records.
- Wording change to expand the ability of a covered entity to disclose PHI to avert a threat to health or safety when harm is "seriously and reasonably foreseeable." (currently it is when harm is "serious and imminent.")
- A pathway has been created for individuals to direct the sharing of PHI maintained in an EHR among covered entities.

Proposed HIPAA Updates

- Covered entities will not be required to obtain a written acknowledgment from an individual that they have received a Notice of Privacy Practices.
- HIPAA-covered entities will be required to post estimated fee schedules on their websites for PHI access and disclosures.
- HIPAA-covered entities will be required to provide individualized estimates of the fees for providing an individual with a copy of their own PHI.
- The definition of healthcare operations has been broadened to cover care coordination and case management.

Proposed HIPAA Updates

- Covered healthcare providers and health plans will be required to respond to certain records requests from other covered healthcare providers and health plans when individuals direct those entities to do so when they exercise the HIPAA right of access.
- Covered entities will be permitted to make certain uses and disclosures of PHI based on their good faith belief that it is in the best interest of the individual.
- The addition of a minimum necessary standard exception for individual-level care coordination and case management uses and disclosures, regardless of whether the activities constitute treatment or health care operations.

Challenges for Providers- Policies and Procedures

- The pending HIPAA updates are intended to ease the administration burden on HIPAA-covered entities, although in the short term, the burden will be increased.
- Updates will need to be made to policies and procedures and changes will be required for notices of privacy practices, although there will not, at least, be the requirement to obtain written acknowledgment that the updated NPPs have been received.

Challenges for Providers- Training

- When the final rule is issued, there will be a requirement to change policies and procedures, and that will require retraining of employees.
- HIPAA requires training to be provided to the workforce during or soon after onboarding, and after any material change in policies and procedures.

Challenges for Providers- Access Issues

- **Improved access to medical records could pose problems for healthcare providers, who will need to ensure they have sufficient staffing and efficient procedures for providing copies of records, as the time frame for providing those records will be shortened from 30 days to 15 days.**
- **The definition of EHRs has also been updated to include billing records, and these will need to be provided to patients who request a copy of their PHI.**
  - **That has the potential to make it more time-consuming to provide copies.**
- Another of the changes related to patient access is the requirement to allow patients to take notes and photographs of their PHI.
  - There will need to be designated places where patients can inspect their PHI privately and, if required, take photographs of their PHI.

Part 2 Proposed Rule

- Stems from Section 3221 Of the Coronavirus Aid, Relief and Economic Security (CARES) Act, March 27, 2020.
- Required HHS Secretary to align certain aspects of Part 2 with HIPAA and the HITECH Acts.
- Part 2 originally implemented in 1975 with very good intentions.
- Over the years, has created a lot of obstacles in treating patients with SUD or addiction issues.
  - Patient consent was basically required for each disclosure or re-disclosure, even for care coordination.

Part 2 Proposed Rule

- Notice of Proposed Rule Making (NPRM) – December 2, 2022
  - Comments due by January 31, 2023
  - **Still in rule-making process**
- One of the biggest changes under the CARES Act was to permit Part 2 programs to share SUD treatment records for treatment, payment and health care operations (TPO) based on a single patient consent.
- Implements patient rights similar to HIPAA and requires implementation of other administrative requirements.

Telehealth

- Public health emergency (PHE) first declared on January 31, 2020.
- PHE expired May 11, 2023.
- Providers furnishing telehealth and related services should take inventory of any flexibilities that are currently in use, and develop a plan to bring operations into full compliance with the post-PHE rules.
- Following the termination of the PHE, all telehealth services will be required to be provided through HIPAA-compliant platforms, including the use of FAA with telehealth technology vendors.
- OCR has issued additional guidance related to the use of audio only telehealth platforms.

Telehealth

OCR Providing 90-Day Transition For Clinicians To Comply With HIPAA Telehealth Rules After End Of COVID-19 PHE

Healthcare Finance News (4/13, Morse) reports, "The Office of Civil Rights is providing a 90-day transition period for" clinicians following the end of the COVID-19 public health emergency "to come into compliance with the HIPAA Rules regarding telehealth, according to the Department of Health and Human Services OCR." The agency said it will "continue to exercise its enforcement discretion and not impose penalties on covered" clinicians "for noncompliance during the 90 - day transition period."

Telehealth

	Top 10 "No Nos" to Watch Out for Post PHE
10	Having phone conversations with patients in public spaces and/or using a speakerphone
9	Initiating telehealth visits with patients using shared/family devices
8	Communicating health information with patients using unencrypted email
7	Texting with patients using consumer messaging apps
6	Conducting telehealth visits on mobile devices over VOIP or a public WI-FI network

Source:
https://telehealthresourcecenter.org/news/preparing-for-the-end-of-the-phe-and-the-end-of-hipaa-enforcement-discretion/.

Telehealth

	Top 10 "No Nos" to Watch Out for Post PHE
5	Having no mechanism for verifying patient identity and/or portal account log-in
4	Conducting telehealth visits using unencrypted consumer video platforms
3	Conducting visits on a telehealth platform without a business associates agreement
2	Not asking/documenting who is in the room with the patient during a telehealth visit
1	Not disclosing who is in the room with the provider during a telehealth visit

Source:
https://telehealthresourcecenter.org/news/preparing-for-the-end-of-the-phe-and-the-end-of-hipaa-enforcement-discretion/.

OCR Proposes Rule – Reproductive Health

- Currently, the HIPAA Privacy Rule permits but does not *require* HIPAA-covered entities to provide reproductive health information to law enforcement.
- April 12, 2023 announcement to enhance privacy protections and strengthen patient-provider confidentiality by prohibiting disclosures of reproductive health information to investigate or prosecute patients, providers and others involved in the provision of legal reproductive health.

OCR Proposes Rule – Reproductive Health

- The **proposed** rule will prohibit disclosures of reproductive health care information for:
  - Criminal, civil, or administrative investigations into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating reproductive health-care where such health care is lawful under the circumstances in which it is provided.
  - The identification of any person for the purpose of initiating such investigations or proceedings.

OCR Proposes Rule – Reproductive Health

- The restrictions will apply in the following situations:
  - Reproductive health care is sought, obtained, provided, or facilitated in a state where the health care is lawful **and** outside of the state where the investigation or proceeding is authorized.
  - Reproductive health care that is protected, required, or expressly authorized by federal law regardless of the state in which such health care is provided.
  - Reproductive health care that is provided in that state where the investigation or proceeding is authorized **and** is permitted by the law of the state in which such health care is provided.

Record Retention

- OAC 310:667-19-14 "Medical records shall be retained a minimum of five (5) years beyond the date the patient was last seen or a minimum of three (3) years beyond the date of the patient's death. Records of newborns or minors shall be retained three (3) years past the age of majority."
- HIPAA requires 6 years.

Record Retention

- OBMLS document:
  - Adult: 10 years from the last patient visit
  - Minor: After the patient reaches age 20 or 10 years from the last visit, whichever is longer.
  - Deceased patient: 6 years past date of death.
- Liability insurer recommendations/preferences?

Legal Medical Record (LMR) v. Designated Record Set (DRS)

- Defining the "medical record" used to be so simple.
- It was the paper chart.
- The paper chart was synonymous with the LMR. The paper chart was the LMR.

LMR v. DRS

- Now, it's not so simple.
- The use of technology for recording patient information has complicated things, as well as new regulatory definitions and requirements.

LMR v. DRS Myths

- **Neither** of the following statements are true:
  - A patient's electronic health record is the LMR. (No.)
  - Patient-specific record printouts to paper or disc are equivalents to the paper chart of the 1980s. (No.)

LMR v. DRS Definitions

- DRS
  - "A group of records maintained by or for a covered entity that may include patient medical and billing records. . . Or information used in whole or in part to make care-related decisions."
  - 45 CFR 164.501

LMR v. DRS Definitions

- LMR
  - AHIMA defined: [t]he legal business record generated at or for a healthcare organization and is the record that would be released upon request.
- The LMR is a subset of the DRS.

LMR v. DRS Definitions

- The legal medical record is typically used when responding to formal requests for information for evidentiary purposes.

LMR v. DRS Definitions

- The legal medical record is typically used when responding to formal requests for information for evidentiary purposes.

Records included in **both** DRS and LMR

- **Clinical Record**
  - History and physical
  - Orders
  - Progress notes
  - Lab reports
  - Vital signs
  - Assessments
  - Consults
  - Clinical reports
  - Authorizations and consents

Records included in **both** DRS and LMR

- **Source Clinical Data**
  - X-rays
  - Images
  - Fetal strips
  - Videos
  - Pathology slides

Records included in DRS and **possibly** LMR

- **External Records and Reports**
  - External records referenced for patient care: other providers records, records provided upon transfer
  - Patient generated records
  - Personal health records
- **Two schools of thought on LMR inclusion.**
  - Can't attest to how outside records created.

Records included in DRS **only**

- **Committee Reports (of patient-specific care decisions)**
  - Ethics committee or tumor board, if deciding on a course of treatment for an individual patient
  - Note: documentation of findings could be reported in the patient's medical record and other privileges may apply.

Records included in DRS **only**

- **Administrative and Financial**
  - Super bills encounter forms
  - Remittance advice
  - Case management records

Records **NOT** included in either the DRS or LMR

- **Secondary/Administrative and Statistical**
  - Tumor registries data
  - QI/QM reports and abstracts
  - Statistical data
  - Committee minutes (not patient-specific treatment related)

Documents Outside of DRS and LMR

- **Health information generated, collected, or maintained for purposes that do not include decision making about the patient**.
  - Data collected and maintained for
    - Research
    - Peer review
    - Performance improvement.
  - Appointment and surgery schedules
  - Birth and death registers
  - Surgery registers
  - Diagnostic or operative indexes
  - Duplicate copies of information that can also be located in the medical or billing records.

Documents Outside of DRS and LMR

- **Psychotherapy notes**
- **Information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding**
- **CLIA**
  - Requisitions for laboratory tests
  - Duplicate lab results when the originals are including in patients record
- **Employer records**
  - Pre-employment physicals
  - Results of tests maintained by infectious disease nurse

Documents Outside of DRS and LMR

- Business associate records that meet the definition of DRS but are duplicate
- Education records
- Source (raw) data interpreted or summarized in the medical record
  - Pathology slides
  - Diagnostic films
  - Electrocardiogram tracings from which interpretations are derived.

Documents Outside of DRS and LMR

- Versions
- Metadata
- Audit trails
- Pending reports
  - P

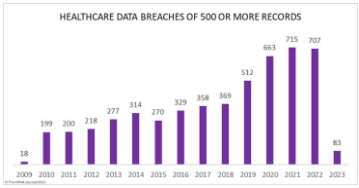
Security - Cyberattacks

94% of Organizations Experienced a Cyberattack in 2022

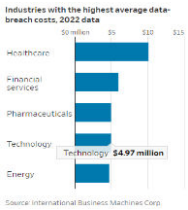
- Posted By HIPAA Journal on Apr 7, 2023

Almost all organizations experienced at least one cyberattack in the past 12 months, according to new research published by Sophos in its State of Cybersecurity 2023 Report. The findings come from an independent study of 3,000 leaders with responsibility for cybersecurity across 14 countries, including the United States. 94% of respondents said they had to deal with at least one cyberattack on their organization in the past 12 months.

HIPAA Data Breaches



Security – Cost of Breaches



Cybersecurity

Health Care Organizations Appear More Reactive Than Proactive In Terms Of Cybersecurity, Survey Indicates

HealthIT Security (4/25, McKeon) reports, "KLAS, the American Hospital Association and health care risk management solutions company Censinet released the much-anticipated first wave of results of its Healthcare Cybersecurity Benchmarking Study," which is "based on responses from 48 health care organizations of varying sizes" and asked "questions focused on measuring adherence to the guidelines recommended by the NIST Cybersecurity Framework (NIST CSF) and the Health Industry Cybersecurity Practices." Regarding "maturity with the NIST CSF's five core functions, survey results indicated that many health care organizations still operate reactively rather than proactively when it comes to cybersecurity." In particular, "the results showed low coverage in the areas of Supply Chain Risk Management, Asset Management, and Risk Management."

Cybersecurity Act of 2015

Section 405(d)

- CSA Section 405 – Improving Cybersecurity in the Health Care Industry
  - Section 405(b): Health care industry preparedness report
  - Section 405(c): Health care industr7 cybersecurity task force
  - **Section 405(d):** Aligning health care industry security approaches
- https://www.phe.gov/Preparedness/planning/405d/Documents/CSA-405d-Overview-508.pdf.

CSA Section 405(d) Legislative Language

- The Secretary shall establish, through a collaborative process with . . . Health care industry stakeholders. . . [federal agencies], a common set of **voluntary, consensus-based, and industry-led** guidelines, best practices, methodologies, procedures, and processes that-

CSA Section 405(d) Legislative Language

- (A) Serve as a resource for **cost-effectively reducing cybersecurity risks** for a range of health care organizations;
- (B) Support **voluntary adoption and implementation** efforts to improve safeguards to address cybersecurity threats;
- (C) Are consistent with –
  - (i) . . . The National Institute of Standards and Technology Act;
  - (ii). . . HIPAA ; and
  - (iii) . . .HITECH Act; and
- (D) Are **updated** on a **regular basis** and **applicable to a range of health care organizations**.

HHS 405(d)

https://405d.hhs.gov/.

HHS 405(d)

- **CYBER SAFETY IS PATIENT SAFETY**
  - **What we do**
  - The 405(d) Program is focused on providing the healthcare & public health (HPH) sector with impactful resources, products, and tools to raise awareness and strengthen the sector's cybersecurity posture against cyber threats. This action drives behavioral change and move towards consistency in mitigating the most relevant cybersecurity threats to the sector with resources like HICP (Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients) and the Hospital Resiliency Landscape Analysis.

HHS 405(d)

- **CYBER SAFETY IS PATIENT SAFETY**
  - **Who we are**
  - The 405(d) Program is a collaborative effort between industry and the federal government to align healthcare industry security practices to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare and public health (HPH) sector's cybersecurity posture against cyber threats. As the leading collaboration center of the Office of the Chief Information Officer/Office of Information Security, the 405(d) Program is focused on providing the HPH sector with useful and impactful resources, products, and tools that help raise awareness and provide vetted cybersecurity practices, which drive behavioral change and move towards consistency in mitigating the most relevant cybersecurity threats to the sector.

Task Group Work Product

- Developed three documents – a main document and two technical volumes.
- The main document examines cybersecurity threats and v8ulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.
- *Technical Volume 1* discusses the 10 cybersecurity practice es for **small** healthcare organizations.
- *Technical Volume 2* discusses these 10 cybersecurity practices for **medium and large** healthcare organizations.

Top 5 Threats

- **Social Engineering**
  - Tricking you into giving out personal information.
- **Ransomware**
- **Loss or Theft of Equipment or Data**
- **Accidental, Intentional, or Malicious Data Loss**
- **Attacks Against Network Connected Medical Devices**

10 Mitigating Practices

HICP's 10 Mitigating Practices

- As presented in Technical Volume 1 and Technical Volume 2, the 405(d) Task Group identified 10 Cybersecurity Practices ranging from personnel training and awareness to the development and implementation of new processes, the acquisition and customization of new technology, and, ultimately, to fostering a consistent, robust, and continually updated approach to cybersecurity.

10 Mitigating Practices

1. Email Protection Systems
2. Endpoint Protection Systems
3. Identity and Access Management
4. Data Protection and Loss Prevention
5. IT Asset Management
6. Network Management
7. Vulnerability Management
8. Security Operations Center & Incident Response
9. Network Connected Medical Device Security
10. Cybersecurity Oversight and Governance

10 Mitigating Practices

- The Practices introduced in this publication strengthen cybersecurity capabilities in health care organizations by:
  - Enabling organizations to evaluate and benchmark cybersecurity capabilities effectively and reliably
  - Sharing knowledge, common practices, and appropriate references across organizations to improve cybersecurity competencies
  - Enabling organizations to prioritize actions and investments—knowing what to ask—to improve cybersecurity

Code Dark

Code Dark: Children's Hospital Strives to Minimize Impact of Hacks

At Children's National Hospital, code dark means a scramble to unplug or turn off internet-connected devices as soon as possible

Hospitals have codes for everything from patient emergencies to hurricanes. Now, Children's National Hospital in Washington, D.C., has one for cyberattacks.
PHOTO: HANNAH BEIER/REUTERS

Code Dark

- Washington, D.C.-based Children's National Hospital has implemented a code that signals staff to unplug or turn off internet-connected devices to mitigate cyberattacks, *The Wall Street Journal* reported Aug. 3.
- Nurses, physicians or staff members who see something suspicious on a technology device report it to the hospital security staff, who then calls "code dark." The code signals technology specialists to begin working on securing the hospital's network while other employees shut down machines near them.
- "If we call a code dark, the entire hospital knows to disconnect devices anywhere they can," Nathan Lesser, chief information security officer of Children's National, told the newspaper. "And then suddenly, we have this additional perimeter. We can reduce the blast radius of malicious code running rampant across our network."
- Mr. Lesser said due to the increase of attacks on healthcare facilities, Children's National Hospital has begun to ramp up its defenses.
- He said the hospital now has detailed instructions on how to power down devices, which include pulling a power or network cord as a last resort.
- The health system has also created training documents with photos of what different cables look like with affixed reminder labels on machines such as monitors and network-connected devices. In addition, all hospital staff members carry cards with code dark steps on lanyards.

Code Dark

Biggest Lessons from Biggest HIPAA Breaches 2022.

- "One notable observation from the biggest HIPAA breaches of 2022 is the number that occurred at business associates of HIPAA-covered entities."
  - https://www.hipaajournal.com/editorial-lessons-from-biggest-hipaa-breaches-of-2022/.
- **Business Associate Risks Must be Managed**.

Incident Response.

- **In June 2023, the Healthcare & Public Health Sector Coordinating Councils issued:**
  - **Coordinated Healthcare Incident Response Plan**

Increased Enforcement- No snooping!

- **Georgia Physician Sentenced to Probation for Unauthorized Medical Record Access (March 31, 2023)**
- A Georgia physician avoided jail time for a HIPAA violation as part of a plea deal . He will also pay $1,000.00 fine and court costs.
- Dr. Brent Harris, family physician, owns several businesses including a school.
- An incident happened at the school involving the son of a nurse, Amy Hicks.
- Dr. Harris accessed the medical record of the child even though he was not the child's physician and looked specifically for information about the parents, Amy and Brett, in particular medication information.
- Dr. Harris used the prescription information to file a nursing board complaint against Amy which was later determined to be unfounded.

Increased Enforcement- No snooping!

Local Hospital To Pay $240K To Settle HIPAA Violation Allegations

Bloomberg Law (6/15, Subscription Publication) reports, "Yakima Valley Memorial Hospital will pay $240,000 and provide additional relief to settle allegations of HIPAA violations in Yakima, Wash., according to the Department of Health and Human Services on Thursday." Data show that "in 2018, 23 hospital security guards allegedly used their login credentials to access patient medical records without a job-related purpose. The information included names, dates of birth, medical record numbers, addresses, treatment notes, and insurance information."

Meta Pixel

- **Is your healthcare facility using Meta Pixel?**
-
- Hospitals across the country are being named as defendants in class action lawsuits asserting violations of HIPAA and other privacy laws as a result of the installation and use of Meta Pixel on their websites. On July 10, a class action lawsuit was filed against one of our Oklahoma health systems, INTEGRIS Health. In very general terms, these class action lawsuits allege that the hospitals websites are collecting and sharing protected health information with social media platforms. For example, one lawsuit against hospitals in Louisiana asserts that when patients made appointments on the hospital websites, Facebook's Pixel code could access their private medical data, such as their medical conditions, medications, and doctor's name. The information was then used to target ads to those patients on their social media accounts. Meta Pixel is a tool used to track website user interactions, using JavaScript code.
-

Artificial Intelligence

- **Privacy and artificial intelligence: challenges for protecting health information in a new era**
  - Blake Murdoch
  - *BMC Medical Ethics* **volume 22**, Article number: 122 (2021) Cite this article
- **MedPro publication, "Artificial Intelligence Risks: Data Privacy and Security"**
  - https://www.medpro.com/artificial-intelligence-risks-privacysecurity.

Questions

- **THANK YOU!**

- **Cori Loomis, JD**
- **cori@christensenlawgroup.com**
- **Follow me on LinkedIn**